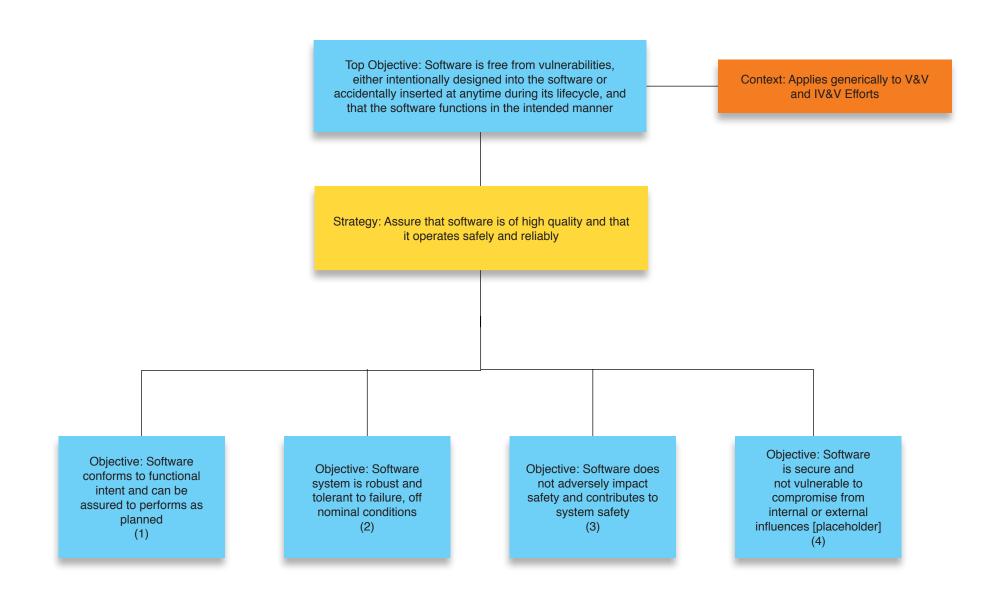
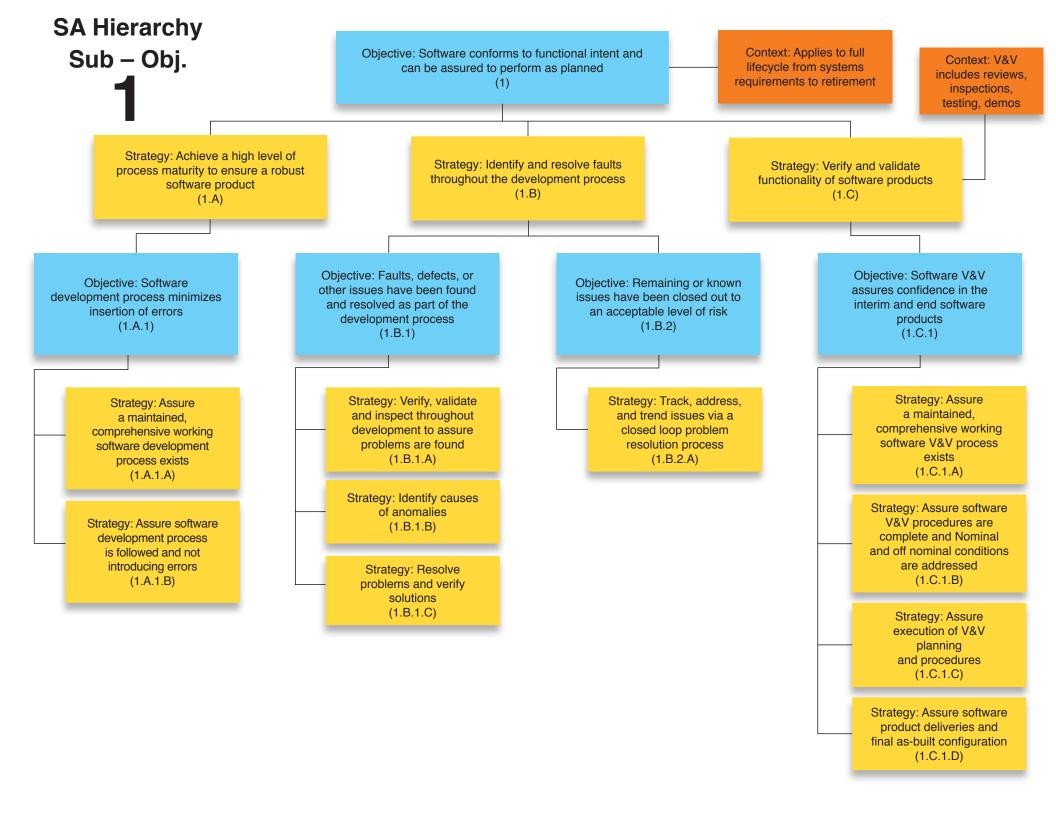
Software Assurance Objectives Hierarchy

SA Objectives Hierarchy – Top Level





SA Hierarchy Sub – Obj.

2

Objective: Software system is robust and tolerant to failure, off nominal conditions

(2)

Strategy: Assure that software is developed in a robust manner, which decreases/eliminates errors, and includes necessary design features to prevent failures and off-nominal conditions from compromising ability to accomplish mission objectives

(2.A)

Objective: Areas of weakness are known and addressed to the proper level (2.A.1)

Strategy: Participate in system analysis and design to determine areas of weakness, suggesting where software design can improve system operability (2.A.1.A)

Strategy: Identify, classify, collect, trend and report defect metrics (2.A.1.B)

Strategy: Analyze metrics, requirements, and design to predict and address problem areas (2.A.1.C)

Strategy: Analyze for software vulnerabilities and recommend design strategies (2.A.1.D) Objective: Has multiple means of accomplishing functions that are critical to mission objectives (2.A.2)

> Strategy: Determine appropriate level for functional redundancy between system and software (2.A.2.A)

> Strategy: Assure appropriate software functional redundancy (2.A.2.B)

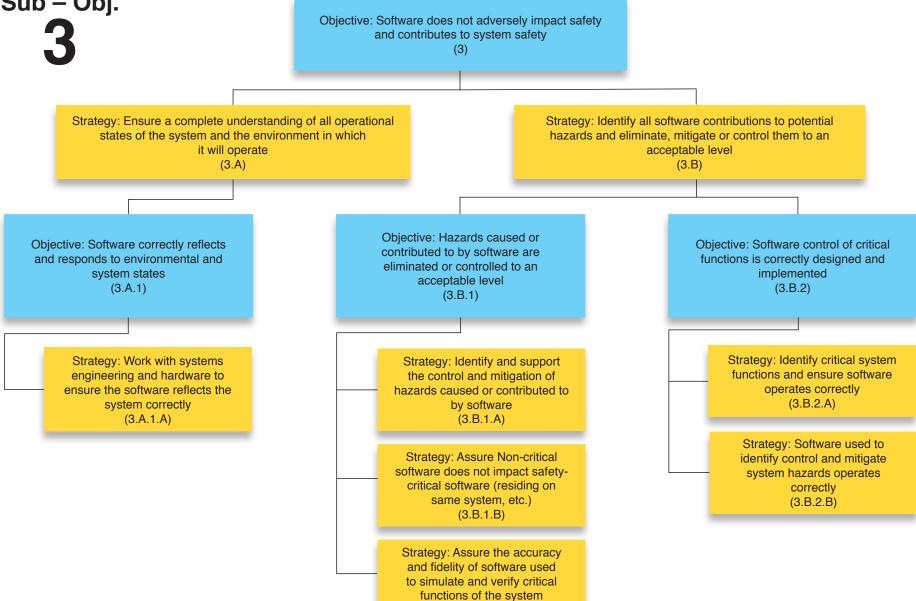
Strategy: Design in appropriate software architecture to meet and maintain critical functions (2.A.2.C) Objective: Pathways for fault propagation or combination through software interfaces are limited (2.A.3)

Strategy: Design in protective barriers to prevent software from propagating system faults (system includes software, hardware, and human interface) (2.A.3.A)

Objective: Software is able to recover from anomalies affecting functionality (2.A.4)

> Strategy: Provide fault management (detection, isolation, recovery) capabilities (2.A.4.A)

SA Hierarchy Sub – Obj.



(3.B.1.C)